

The RPOST server is involved in every step in applicant's method. This is recited in each of the claims being prosecuted in this application. For example, each claim recites, in the preamble, language such as "the steps at the server of:" In these different steps, the RPOST server either (a) transmits data to a sender or a recipient, (b) receives data from the sender or the recipient or (c) processes data received by the RPOST server from the sender or the recipient. An example of step (a) in the RPOST system is step (2) in the flow chart constituting Exhibit A. In this step, the RPOST server transmits the message to the destination address. An example of step (b) in the flow chart constituting Exhibit A is step (3) in Exhibit A. In this step, the message passes from the destination address of the recipient to the RPOST server. An example of step (c) in the flow chart constituting Exhibit A is step (4) in Exhibit A. In this step, the RPOST server maintains the message and additionally provides an encrypted hash of the message.

Exhibit B is a flow chart of method 1 in Barkan. It is similar in a few respects to Exhibit A in the RPOST system but the results are quite different. As will be seen in Exhibit B, various steps are performed by the user 1, the user 2 and a distribution center 63. For example, in step 1 of Exhibit B, user 1 sends to distribution center 63a first message intended for user 2 and asks center 63 to provide user 1 with the public key of user 2. In step 2 in Exhibit B, distribution center 63 encrypts the public key of user 2 with the private key of the distribution center 63. In step 3 in Exhibit B, the encrypted private key of distribution center 63, encrypted with the public key of user 2, is transmitted from the distribution center 63 to the user 1.

Exhibit C is a flow chart constituting a bare bone outline of Exhibit A. It is bare bone because it shows numerically what the different steps in Exhibit A are without specifying what these steps are. As will be seen, steps 1 and 7 are transmissions of data from the sender to the RPOST server; step 5 is a transmission from the RPOST server to the sender; steps 4, 6, 8 and 9 involve the processing of information at the RPOST server; step 2 involves the transmission of information from the RPOST server to the destination address of the recipient; and step 3 involves the transmission of data from the destination address of the recipient to the RPOST server. Thus, the RPOST server is involved in all of steps 1-9 either in transmitting, receiving or processing information.

In like manner, Exhibit D is a flow chart constituting a bare bone flow chart of Exhibit B. It is bare bone because it shows numerically what the different steps are in Exhibit B without designating what these different steps are. As shown in Exhibit D, delivery center 63 is not involved in steps 1, 4, 5 and 7; user 1 is not involved in steps 4-7; and user 2 is not involved in steps 1-5. Thus, none of the user 1, the user 2 and the delivery center 63 is involved in all of steps 1-7. This is in contrast to Exhibit C where the RPOST server is involved in every step.

There are ten (10) methods in Barkan. In each of methods 2-10, none of the members is involved in all of the method steps.

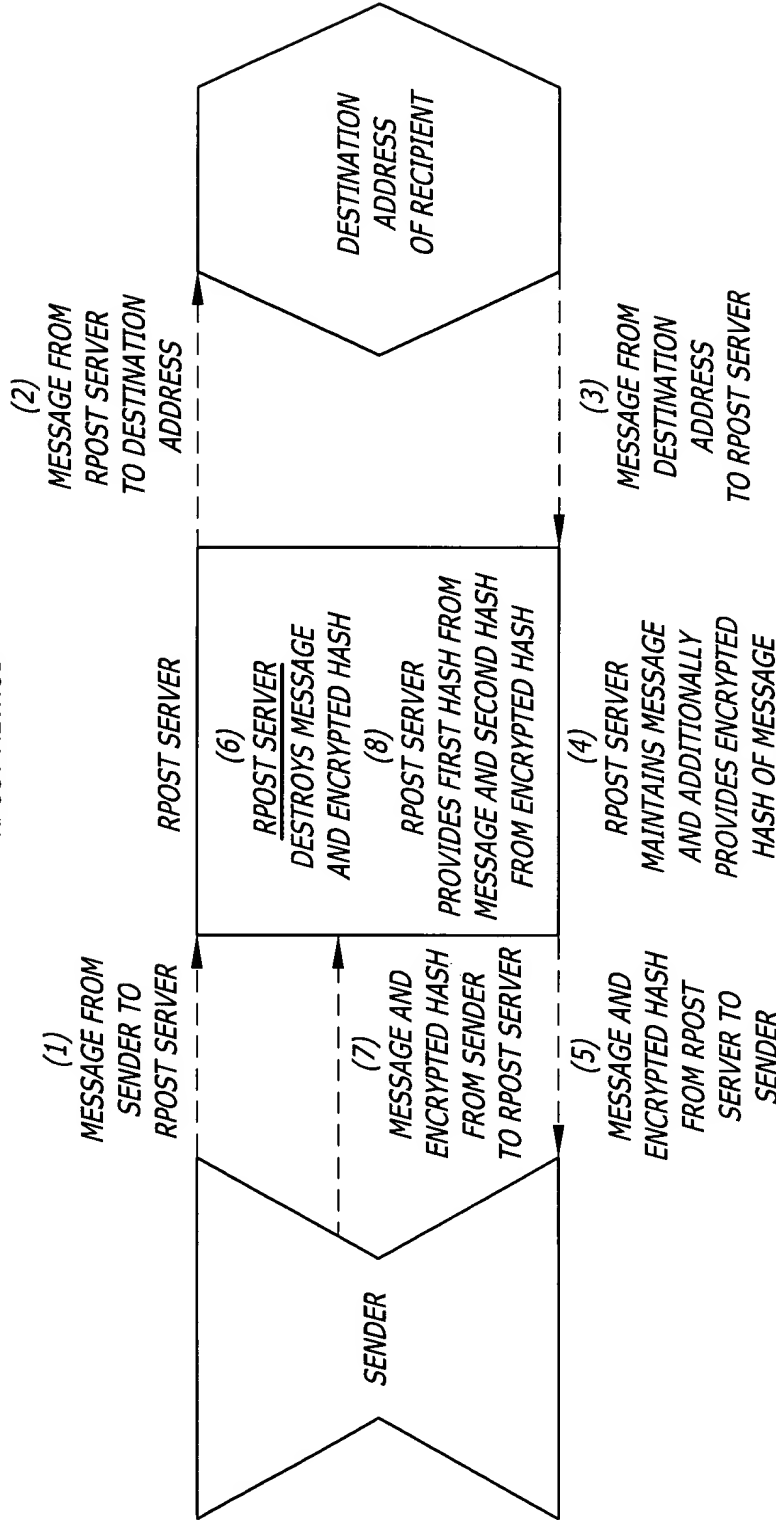
Respectfully submitted,
FULWIDER PATTON LEE & UTECHT, LLP

By: Ellsworth R. Roston
Ellsworth R. Roston
Registration No. 16,310

Howard Hughes Center
6060 Civic Center Drive, Tenth Floor
Los Angeles, CA 90045
Telephone: (310) 824-5555
Facsimile: (310) 824-9696
Customer No. 24201

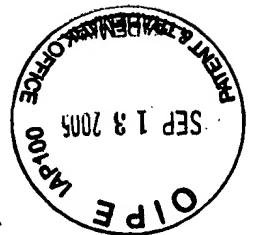
ERR:dmc

RPOST METHOD



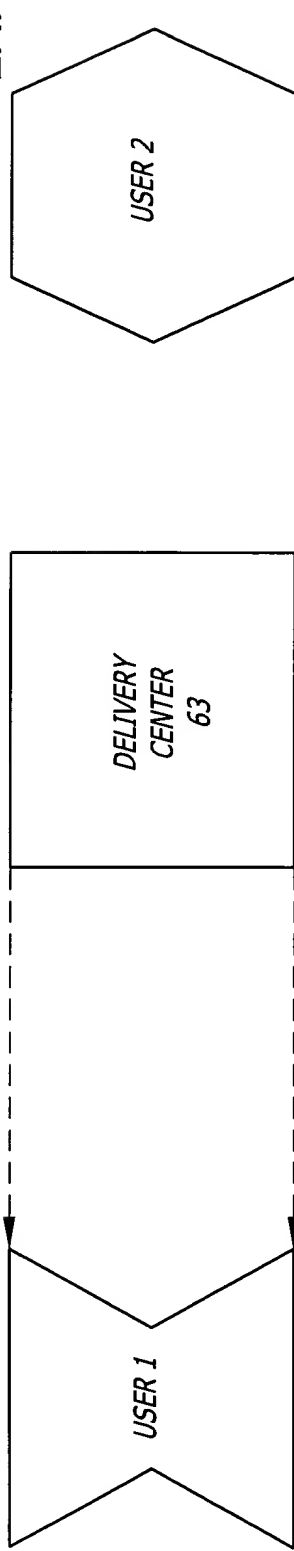
(9)
RPOST SERVER COMPARES FIRST AND SECOND HASHES. IF HASHES ARE IDENTICAL, RPOST SERVER AUTHENTICATES MESSAGE. IF HASHES ARE NOT IDENTICAL, RPOST SERVER DOES NOT AUTHENTICATE MESSAGE

EXHIBIT A



BARKAN METHOD

EXHIBIT B



(1)

USER 1 SENDS
TO DISTRIBUTION
CENTER 63 A MESSAGE
INTENDED FOR
USER 2 AND ASKS
CENTER 63 FOR
PUBLIC KEY OF USER 2

(2)

CENTER 63 ENCRYPTS
PUBLIC KEY OF
USER 2 WITH PRIVATE
KEY OF CENTER 63

(4)

USER 1 DECRYPTS
PRIVATE KEY OF
CENTER 63 TO OBTAIN
ENCRYPTED PUBLIC
KEY OF USER 2

(3)

ENCRYPTED PRIVATE KEY
OF CENTER 63, ENCRYPTED
WITH PUBLIC KEY OF
USER 2, SENT FROM CENTER 63
TO USER 1

(5)

USER 1 ENCRYPTS
FIRST MESSAGE WITH
PUBLIC KEY OF
USER 2 TO CREATE
A SECOND MESSAGE

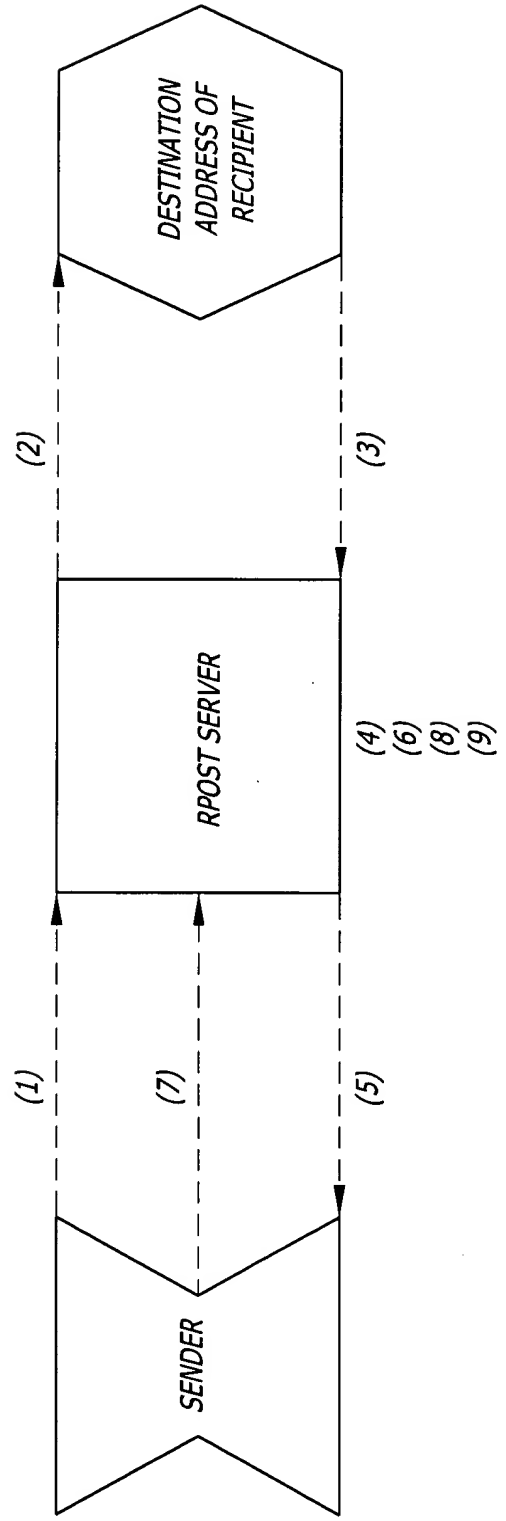
(6)

USER 1 SENDS THE SECOND
MESSAGE WITH THE PUBLIC
KEY OF USER 2 TO USER 2

(7)

USER 2 DECRYPTS THE SECOND
MESSAGE WITH THE PRIVATE
KEY OF USER 2 AND OBTAINS
THE MESSAGE

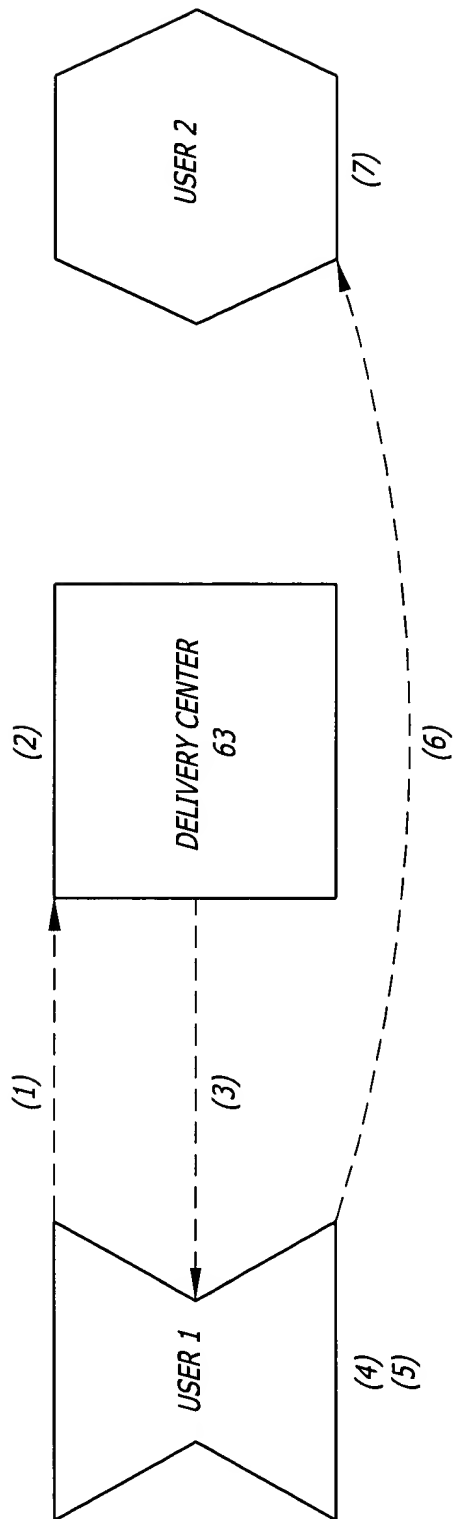
RPOST METHOD



RPOST SERVER IS INVOLVED
IN EVERY ONE OF STEPS 1-9

EXHIBIT C

BARKAN SYSTEM



DELIVERY CENTER 63
NOT INVOLVED IN STEPS
1, 4, 5, 6 AND 7

USER 1 NOT INVOLVED IN
STEPS 2, 6, 7

USER 2 NOT INVOLVED
IN STEPS 1-5

EXHIBIT D

NONE OF USER 1, DELIVERY CENTER
63 AND USER 2 INVOLVED IN ALL OF STEPS
1-7



OPERATIVE STEPS IN RPOST METHOD

1. Sender submits a message to the RPOST server for transmission by the RPOST server to a destination address of a recipient.
2. RPOST server transmits the message to the destination address of the recipient.
3. The message is returned from the destination address to the RPOST server.
4. The RPOST server maintains the message and additionally provides an encrypted hash of the message.
5. The RPOST server transmits the message and the encrypted hash to the sender. The RPOST server instructs the sender to save the message and the encrypted hash so that the RPOST server can authenticate the message at a subsequent time if and when requested by the sender. The RPOST server informs the sender that the sender will have the only copy of the message and the encrypted hash because the RPOST server intends to destroy its copy of the message and the encrypted hash.
6. The RPOST server destroys its copy of the message and the encrypted hash.
7. At a subsequent time, the sender desires to have the message authenticated. The sender sends the message and the encrypted hash to the RPOST server.
8. The RPOST server provides a hash of the message from the sender to obtain a first hash and decrypts the encrypted hash from the sender to obtain a second hash.
9. The RPOST server compares the two (2) hashes. If the hashes are identical, the RPOST server authenticates the message. If the two (2) hashes are not identical, the RPOST server refuses to authenticate the message.

ADVANTAGES OF RPOST METHOD

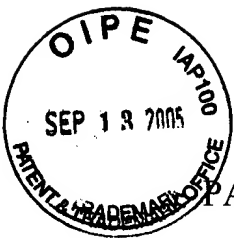
1. The RPOST server does not store the message or the encrypted hash of the message. This is important because the RPOST server would be overwhelmed by enormous quantities of messages and encrypted hashes from all of the senders if the RPOST server saved the message.
2. The sender stores the message and the encrypted hash of the message and requests authentication of a message that the RPOST server has provided to the destination address of recipient. It is accordingly appropriate that the sender stores the message and the encrypted hash of message.
3. There is a seamless flow of information in the RPOST method. In other words, there is no backtracking. See flow diagram (Exhibit A) on separate sheet. This means that the information flows in a first closed loop between the RPOST server and the destination address, and in a second closed loop between the sender and the RPOST server, without any backtracking.
4. All of the successive steps in applicant's system start, stop or occur at the RPOST server. This means that the RPOST server is involved in every step of the method recited in applicant's claims.



OPERATIVE STEPS IN BARKAN METHOD

METHOD 1 IN INTERNATIONAL APPLICATION PUBLIC NUMBER WO98/17042 OF BARKAN:

1. User 1 prepares a first message, intended to be submitted to user 2, and sends a report through the internet to a distribution center 63 and asks for the public key of user 2.
2. Center 63 encrypts the public key of user 2 with the private key of the center 63.
3. Center 63 sends the encrypted public key of the user 2 with the private key of the center 63 through the internet to the user 1.
4. User 1 decrypts the encryption of the center 63 to obtain the encryption of the public key of the user 2.
5. User 1 encrypts the first message with the public key of the user 2 to create a second message.
6. User 1 sends the second message through the internet to the user 2.
7. User 2 decrypts the second message with the public key of user 2 to obtain the first message.



PATENTABLE DIFFERENCES BETWEEN APPLICANT'S METHOD AND BARKAN'S METHOD AS RECITED IN APPLICANT'S CLAIMS

1. In applicant's method, the RPOST server provides the authentication of the message. In Barkan's method, the recipient of the message provides the authentication of the message. In other words, when user 1 transmits a message to user 2, user 2 authenticates the message.

2. In applicant's method, the message being processed is unencrypted. In Barkan's method, the message being processed is encrypted. In other words, whenever the message is transmitted in Barkan from a first user (e.g., user 1) to a second user (e.g., user 2), the message is initially encrypted at the first user and is decrypted at the second user.

3. Since the message is transmitted without any encryption in the RPOST method and since the RPOST server authenticates the message, the RPOST server provides a comparison between the message and a representation of the message. In the RPOST method, the representation is an encrypted hash which is generated by the RPOST server from the message. To authenticate the message, the RPOST server produces a first hash of the message and decrypts the encrypted hash to provide a second hash of the message. The RPOST server then compares the two (2) hashes. When the two (2) hashes are identical, the RPOST server authenticates the message. When the two (2) hashes are not identical, the RPOST server does not authenticate the message.

The Barkan method authenticates the message in a completely different way. In the Barkan method, the sender (e.g., user 1) transmits the message to the recipient (e.g., user 2) with an encryption individual to the user 2. In this way, the recipient (e.g., user 2) authenticates the message when it decrypts the message.

4. In the RPOST method, the RPOST server is central to the system. It is the driving force of the system. It provides a communication between the sender and the recipient. It produces the encrypted hash of the message. It operates upon the message and the encrypted hash to provide an authentication of the message.

The central importance of the RPOST method is recited in applicant's claims. This may be seen from the fact that all of the claims being prosecuted in this application recite that all of the recited steps are provided at the RPOST server.

In the Barkan method, the distribution center 63 is not involved in steps 4, 5 and 6. Furthermore, none of the user 1, the user 2 and the delivery center 63 is involved in all of the steps in method 1 in Barkan.

In the Barkan method, the distribution center 63 is passive. It is not involved in the operation of the method. It serves only to indicate to one of the users what is the key encryption of the other user.

5. Barkan discloses ten (1) different methods in his patent application. Each method is distinct from the others. The Examiner has rejected all of the claims on the basis of Barkan as the primary reference. However, the Examiner has not rejected any single one of the claims by citing steps only from a single one of the ten (10) different methods. Instead, the Examiner has cited steps from more than one (1) of the ten (10) methods against each individual one of the claims. In citing steps from more than one (1) reference against each individual one of the claims, the Examiner has not shown how the different steps from the more than one (1) method in Barkan are combined to form a unified structural combination rather than isolated steps defining an aggregation.

6. Applicant provides a seamless method. This means that there is no backtracking in successive steps in the method. In other words, successive steps in applicant's method are performed in the same location as the previous step or are performed in a successive location. In method 1 of Barkan, step 1 is performed from user 1 to delivery center 63; step 3 is performed from delivery center 63 to user 1; and step 6 is performed from user 1 to user 2. This causes a backtracking to occur in step 6.